APLIKASI PENGAMAN DATA MENGGUNAKAN ALGORITMA RSA (Rivest-Shamir-Adleman)

TUGAS AKHIR

Diajukan Oleh :

DUWI MUJIARTO

NPM : 0734010242

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2012

Judul : APLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITHMA RSA (RIVEST-SHAMIR-ADLEMAN)

Pembimbing I : Ir. Purnomo Edi.S, MP

Pembimbing II : Dr.Ir. Ni Ketut Sari, MT

Penyusun : Duwi Mujiarto

ABSTRAK

Masalah keamanan dan kerahasiaan data dalam suatu komputer merupakan aspek penting yang tidak dapat diabaikan keberadaannya. Apalagi jika data-data tersebut disimpan dalam suatu komputer yang digunakan secara bebas. Hal ini akan menyebabkan semua data yang kita miliki dapat diakses oleh semua orang. Untuk menangani masalah tersebut maka diperlukan suatu aplikasi pengamanan data yang dapat mencegah dan mengamankan data-data yang dimiliki dari para pemakai yang tidak berhak mengaksesnya. Yaitu dengan membuat sistem keamanan file dan folder data. Pada Aplikasi ini menerapkan metode enkripsi sehingga membuat data / file yang kita miliki menjadi lebih sulit untuk dimengerti isinya. Metode tersebut menggunakan algoritma RSA (Rivest-Shamir-Adleman).

RSA merupakan algoritma pertama yang cocok untuk digital signature seperti halnya ekripsi, dan salah satu yang paling maju dalam bidang kriptografi public key. RSA masih digunakan secara luas dalam protokol electronic commerce, dan dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang.

Dalam Skripsi ini penulis, merancang aplikasi dengan menggunakan bahasa pemrograman Delphi. Aplikasi ini menggunakan algoritma RSA, dan menggunakan key untuk menentukan nilai bit proses pengirimannya, prosenya pertama yang dilakukan dari file bertipe text kemudian dienkrip dan menghasilkan berupa bilangan desimal dan bertipe sck kemudian dari file bertipe sck didekrip dan kembali sperti semula bertipe text.

Kata kunci: RSA, Enkripsi, Dekripsi

KATA PENGANTAR

Alhamdulillaahi Robbil ‘Alamin…Puji syukur penulis panjatkan kepada Allah Yang Maha Esa yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan Tugas Akhir ini yang berjudul “APLIKASI PENGAMAN DATA MENGGUNAKAN ALGORITMA RSA (RIVEST-SHAMIR-ADLEMAN) ” tepat pada waktunya.

Tugas Akhir dengan beban 4 SKS ini disusun guna diajukan sebagai salah satu syarat untuk menyelesaikan program Strata Satu (S1) pada program studi Teknik Informatika, Fakultas Teknologi Industri, UPN ”VETERAN” Jawa Timur.

Dengan selesainya Tugas Akhir ini tidak terlepas dari bantuan banyak pihak yang telah memberikan masukan-masukan dan semangat kepada penulis. Untuk itu penulis mengucapkan terima kasih kepada :

1. Orang tua kami tercinta dukungan serta harapan-harapanya pada saat kami menyelesaikan laporan ini. Terima kasih atas kasih sayang dan do’anya.
2. Bapak Ir.Sutiyono, MT selaku Dekan Fakultas Teknologi Industri Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Ibu Dr.Ir. Ni Ketut Sari, MT selaku Ketua Jurusan Teknik Informatika
4. Dosen Pembimbing I Bapak Ir.Purnomo Edy S., MP.
5. Dosen Pembimbing II Dr.Ir. Ni Ketut Sari, MT
6. Teman-teman seperjuangan : Ibet (Gundul), Basori (Mbah), Faris (Phobia), Agus (Menunggu) yang selalu membantuku dan mensupport, Wahyu (Kiyep), Toni (Soto), Rizal (Komeng) selalu membantu semua hal. Rizal (Atenk),

Arpin, Sektian, Luky yang selalu menemani di kampus. Dan semua anak TF angkatan 2007 ayo terus dan terus..berjuang rek….

7. Seluruh teman-teman Jurusan Teknik Informatika UPN “VETERAN” Jatim.

Penulis menyadari bahwa masih banyak kekurangan dari laporan Tugas Akhir ini, baik dari materi maupun teknis penyajiannya, mengingat kurangnya pengetahuan dan pengalaman penulis. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan.

Surabaya, 09 Februari 2012

Penulis

DAFTAR ISI

Halaman

KATA PENGANTAR i
DAFTAR ISI iii
DAFTAR TABEL vi
DAFTAR GAMBAR vii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan 3
1.5 Manfaat Sistem Bagi Pengguna 3
1.6 Metodelogi 3
1.7 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 6
2.1 Security..... 6
2.2 Kriptografi..... 6
2.2.1 Algoritma kriptografi..... 7
2.2.2 Tinjauan Matematis 10
2.3 Kriptanalisis..... 14
2.3.1 Embarcadero Dhelpi 2010..... 15
2.3.2 Keuntungan Dhelpi 21
2.4 Alghorithma RSA..... 22
2.4.1 Sejara RSA..... 22
2.4.2 Operasional..... 23
2.4.3 Proses enkripsi pesan 25
2.4.4 Proses dekripsi pesan..... 25
2.5 Sistem kerja RSA..... 27
2.5.1 Contoh Penggunaan Algoritma..... 28

2.5.2 Kode Ascii..... 30
2.5.3 Kecepatan RSA..... 31
2.5.4 Penyerangan waktu..... 31
2.5.5 Penyerangan ciphertex adaptive..... 32
2.6 Distribusi kunci..... 32
2.6.1 Pembangkitan kunci..... 33
2.6.2 Kunci Lemag dan Kunci setengah lemah..... 34
2.7 Mode Operasi..... 35
2.8 Padding schemes..... 36
2.9 Ancaman yang mungkin menyerang RSA..... 37
2.10 Keamanan Algoritma RSA..... 37
2.11 Pertimbangan Teknis dalam Enkripsi RSA..... 39
2.12 Keuntungan dan kerugian RSA..... 40
2.13 Metode Algoritma Vegenere chiper dimensi 3..... 40
BAB III ANALISIS DAN PERANCANGAN 45
3.1 Analisis Permasalahan..... 45
3.2 Alat Dan Bahan Penelitian..... 46
3.3 Desain Penelitian..... 46
3.4 Analisa Permasalahan..... 47
3.5 Diagram Alir sistem..... 49
3.6 Algoritma Pembuatan Kunci RSA..... 50
3.7 Potongan sourcode untuk pembentukan kunci bit 51
BAB IV IMPLEMENTASI DAN PENGUJIAN..... 52
4.1 Implementasi Sistem 52
4.1.1 Impelemtasi Antar Muka..... 52
4.1.2 Form Lokasi 53
4.1.3 Form setting pengaman..... 54
4.1.4 Form lokasi pengiriman data 55
4.1.5 Botton Enkripsi..... 55
4.1.6 Botton Dekripsi..... 57
4.1.6 Botton Bantuan..... 58

4.1.7 Botton Tentang..... 59
4.2. Pengujian progam.....60
4.2.1 Tampilan Menu Utama.....60
4.2.2 Inputan User.....61
4.2.3 Form Lokasi yang dipantau..... 61
4.2.4 File List Box.....62
4.2.5 Form lokasi Pengiriman data..... 62
4.2.6 Isi file Text..... 63
4.2.7 Hasil Enkripsi..... 63
4.2.8 Botton Keluar..... 64
4.2.9 Message Box..... 64
4.2.10 Hasil Uji coba..... 65
BAB V PENUTUP 61
5.1 Kesimpulan 66
5.2 Saran 66
DAFTAR PUSTAKA

DAFTAR TABEL

Halaman

Tabel 2.1	Operasi AND …….....	12
Tabel 2.2	Operasi OR .....….....	13
Tabel 2.3	Operasi XOR	13
Tabel 2.4	Jenis-jenis file dalam delphi.....	21
Tabel 2.5	Kunci pesan untuk mengenkripsi data.....	29
Tabel 2.6	Kode ASCII.....	30
Tabel 2.7	Hasil Uji Coba.....	61

DAFTAR GAMBAR

Halaman

Gambar 2.1 Proses Enkripsi/Dekripsi Sederhana 7

Gambar 2.2 Proses Enkripsi dan Dekripsi Algoritma Kriptografi Simetri 8

Gambar 2.3 Proses Enkripsi dan Dekripsi dengan Dua Kunci yang Berbeda 9

Gambar 2.4 Tampilan awal Delphi..... 17

Gambar 2.5 Daftar komponen palet standard Delphi..... 18

Gambar 2.6 Daftar komponen palet additional..... 18

Gambar 2.7 Daftar komponen palet win 32..... 18

Gambar 2.8 Daftar komponen palet system..... 19

Gambar 2.9 Komponen Palet Dialog..... 19

Gambar 2.10 Membuat aplikasi sederhana dengan Delphi 20

Gambar 3.1 Aktifitas Desain Penelitian..... 43

Gambar 3.2 Diagram Alir Sistem Enkripsi Menggunakan RSA 45

Gambar 4.1 Desain Antar Muka..... 48

Gambar 4.2 Form Lokasi.....……..... 49

Gambar 4.3 Form setting pengaman.....……..... 50

Gambar 4.4 Form Lokasi pengiriman data……..... 51

Gambar 4.5 Botton Enkripsi ……..... 51

Gambar 4.6 Botton Dekripsi..... 53

Gambar 4.7 Botton bantuan..... 54

Gambar 4.8 Form info Bantuan..... 54

Gambar 4.9 Botton Tentang ……..... 55

Gambar 4.10 Form info tentang..... 55

Gambar 4.11 Tampilan menu Utama..... 56

Gambar 4.12 Inputan User ……..... 57

Gambar 4.13 Lokasi yang dipantau..... 57

Gambar 4.14 FileListBox ……..... 58

Gambar 4.15 form Lokasi pengiriman Data ……..... 58

Gambar 4.16 Isi file text ……..... 59

Gambar 4.17 Hasil Enkripsi …..... 59

Gambar 4.18 Button Keluar ……..... 60

Gambar 4.19 MessageBox ……..... 60

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada masa sekarang, komputer dan aplikasi telah berkembang pesat penggunaannya, sehingga dapat dikatakan keberadaannya sangat melekat pada kehidupan sehari-hari, baik itu pekerjaan, hiburan, maupun sesuatu yang pribadi. Tidak hanya di kota besar, kini komputer mulai menyebar hingga ke desa. Dan tidak hanya secara konvensional menggunakan Personal Computer (PC) kini juga bisa menggunakan notebook.

Selama ini dalam pengaturan hak akses, hanya mengandalkan pengaturan account dengan pemberian username dan password. Tentunya, pada masa sekarang ini hal tersebut tidaklah mencukupi, mengingat sebuah user account dapat dicuri ataupun seorang hacker dapat meretas langsung ke dalam sebuah jaringan dan langsung mengambil data-data yang diperlukan.

Adanya potensi tindakan peretasan jaringan ataupun pengambilan user account dapat menyebabkan terjadinya kerawanan kerahasiaan suatu data atau dokumen sehingga diperlukan suatu aplikasi yang dapat mengamankan data, khususnya untuk shared document pada jaringan komputer lokal agar dokumen atau data tersebut hanya dapat dibaca oleh orang yang berhak.

Algorithma RSA merupakan salah satu teknik pengamanan data dengan cara mencocokan public key yang dimiliki oleh pengirim dokumen dan penerima dokumen, yang selanjutnya dilakukan proses penguraian dengan sebuah private

key. Teknik ini sangat membantu proses pengamanan file data, karena hanya orang yang punya private key saja yang dapat menguraikan isi file tersebut.

Berdasarkan uraian tersebut, maka dalam tugas akhir kali ini saya akan membuat aplikasi yang dapat melakukan proses pengamanan data menggunakan algorithma RSA.

1.2. Perumusan Masalah

Rumusan masalah yang digunakan dalam tugas akhir ini adalah :

- Bagaimana membuat aplikasi pengiriman file dilengkapi dengan fitur pengamanan data menggunakan algorithma RSA ?

1.3. Batasan Masalah

Dalam tugas akhir ini batasan masalah yang dipergunakan yaitu :

a. Format file yang dipergunakan sebagai uji coba adalah tipe dokumen (text)
b. Ukuran file 500 MB, lokasi pengiriman berada dalam satu hanya satu lokasi dalam sekali pengiriman.
c. Aplikasi dibangun dengan menggunakan developer embarcadero developer studio 2010
d. Aplikasi dapat berjalan pada sistem operasi Microsoft Windows Vista atau Windows Seven.

1.4. Tujuan

Tujuan yang ingin dicapai pada pengerjaan tugas akhir ini adalah: membuat aplikasi pengiriman file menggunakan algorithma RSA untuk meningkatkan keamanan data baik untuk pengirim maupun untuk penerima

1.5. Manfaat

Adapun manfaat yang ingin diperoleh dari pengerjaan tugas akhir ini adalah dapat membuat perangkat lunak untuk mempermudah pengguna mengamankan data, khususnya dalam lingkungan pekerjaan.

1.6. Metode Penelitian

Adapun metode penelitian yang dipergunakan dalam pengerjaan tugas akhir ini adalah :

1) Studi Literatur

   Mengumpulkan referensi baik dari buku, internet, maupun sumber-sumber yang lainnya yang terkait dengan judul penelitian ini.

2) Studi Kasus

   Mencari contoh-contoh kasus serupa dan hasil ujicoba yang berhubungan dengan permasalahan dalam tugas akhir ini.

1.7. Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, identifikasi masalah, maksud dan tujuan yang ingin dicapai, batasan masalah, metodologi penelitian yang diterapkan dalam memperoleh dan mengumpulkan data, waktu dan tempat penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik masalah yang diambil dan hal-hal yang berguna dalam proses analisis permasalahan.

BAB III ANALISIS DAN PERANCANGAN

Menganalisis masalah dari model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti serta model matematis untuk analisisnya.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Membahas mengenai pengimplementasian aplikasi yang telah dibuat ke perangkat yang akan digunakan serta melakukan pengujian terhadap aplikasi yang telah diimplementasikan tersebut.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir.

DAFTAR PUSTAKA

Berisi tentang referensi-referensi dalam menunjang penulis mengerjakan tugas akhir.